REMARKS

In the Office Action, the Office rejected claims 1, 4, 5, 9, 10, 12-15, 31, 32, 34 and 35 under 35 U.S.C. § 102(e) as being anticipated by U.S. Patent No. 6,256,737 (Bianco). Claims 1, 5, 14, 15 and 31 have been amended, and claims 34 and 35 have been cancelled without prejudice. No new matter has been added as a result of these amendments.

Upon entry of this Preliminary Amendment, claims 1, 4, 5, 9, 10, 12-15, 31 and 32 will remain pending. For the reasons set forth hereinbelow, Applicants respectfully request that the rejections associated with the pending claims be withdrawn.

Claims 1, 4, 5, 9, 10 and 12-15

Applicants submit that independent claim 1 is not anticipated by Bianco, because Bianco fails to disclose each and every element of claim 1. *See* MPEP §2131 (stating that a claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in the single prior art reference). More particularly, Applicants submit that Bianco fails to disclose at least the following limitations of amended claim 1:

- receiving, from a first biometric device, ... first biometric device data indicative of a capability of the first biometric device;

- locating second biometric device data indicative of a capability of the second biometric device;

- determining whether the first biometric device data indicates that the capability of the first biometric device is superior to the capability of the second biometric device; and

- generating upgraded biometric data based on a combination of the registered biometric data and said received biometric data.

Bianco discloses a method for utilizing biometric measurements for the authentication of users to enterprise resources. *See* Bianco at Abstract. Bianco discloses that a biometric server stores collections of biometric templates, biometric policies, biometric groups, biometric device IDs, user IDs, computer IDs and application IDs. *See id.* at 17: 38-41. A unique biometric template is created and stored in the biometric server each time a user enrolls on a different biometric device. *See id.* at 17:41-44. Biometric groups, which represent a way of combining one or more users that need access to the same set of resources, are also stored in the biometric

server. *See id.* at 18:8-11. Each biometric group may be assigned a particular biometric policy that is also stored in the biometric server. *See id.* at 18:18-43. Once it is known which biometric policy will be applied, a biometric template is created for each biometric device associated with the biometric policy by enrolling the user in each device. *See id.* at 19:27-34. Moreover, Bianco teaches that there is one biometric template for each biometric device ID. *See id.* at 24:9-10. As such, Bianco teaches assigning biometric templates based on a biometric group or policy assigned for a particular user and to a particular device.

In contrast, claim 1 requires receiving first biometric device data indicative of a capability of a first biometric device from the first biometric device. Bianco merely teaches receiving biometric measurements, which are used to generate a biometric template. Bianco does not teach or suggest receiving data pertaining to the first biometric device. In particular, Bianco does not teach or suggest receiving data indicative of a capability of a first biometric device.

Moreover, claim 1 requires locating second biometric device data indicative of a capability of the second biometric device. As mentioned above, Bianco merely teaches locating a registered biometric template. Bianco does not teach or suggest locating second biometric device data pertaining to the second biometric device. More particularly, Bianco does not teach or suggest locating second biometric device data indicative of a capability of the second biometric device.

Furthermore, claim 1 requires determining whether the first biometric device data indicates that the capability of the first biometric device is superior to the capability of the second biometric device. Bianco teaches that biometric data may be updated from time to time based on changes in the user's biometric characteristics (due to aging, weight gain or loss, etc.). *See* Bianco at 28:43-52. However, Bianco does not teach or suggest determining whether biometric **device** data indicates that the capability of a first biometric **device** is superior to the capability of a second biometric **device**. Rather, Bianco merely teaches that more current biometric data may indicate a change in a biometric characteristic of a user.

Additionally, claim 1 requires generating upgraded biometric data based on a combination of the registered biometric data and said received biometric data. The Office states that Bianco teaches an equation that combines two values to obtain a TEMP SCORE that is used to authenticate a user via a comparison and that in itself is a combination too. *See* Office Action

-12-

at 3; Bianco at FIG. 21B (2124, 2126). Applicants respectfully disagree. Bianco teaches generating a biometric score from a first device and prompting the user to utilize another device if the biometric score is insufficient to identify a match. The process can repeat until it gets an accurate score or no additional devices are available. *See* Bianco at 30:66-31:25, FIG. 21B. The user is tested on two or more devices either to provide better authentication or to authorize the user if he fails on the first device. As such, the "score" in Bianco represents a biometric matching score. In other words, the score is utilized as part of the matching process. In contrast, claim 1, requires that a biometric match occur first **before considering whether to upgrade the stored biometric data**. If there is no match, the capability of the second device is never considered.

More particularly, Bianco doesn't combine registered biometric data and received biometric data. In FIG. 21 (step 2124), Bianco merely teaches combining authentication scores to generate one authentication score. However, combining authentication scores is completely dissimilar from generating new biometric data to serve as the registered template. Rather, Bianco merely takes the results from one biometric authorization and adds them to the results of another biometric authorization.

Therefore, for at least the reasons set forth hereinabove, Applicants submit that claim 1 is allowable over the Examiner-cited prior art. *See* MPEP §2131. Because claims 4, 5, 9, 10 and 12-15 depend from and incorporate all of the limitations of allowable independent claim 1, Applicants submit that claims 4, 5, 9, 10 and 12-15 are likewise allowable over the Examiner-cited prior art. Accordingly, Applicants respectfully request that the rejections associated with claims 1, 4, 5, 9, 10 and 12-15 be withdrawn.

Claims 31 and 32

Applicants submit that independent claim 31 is not anticipated by Bianco, because Bianco fails to disclose each and every element of claim 31. *See* MPEP §2131. More particularly, Applicants submit that Bianco fails to disclose at least the following limitations of amended claim 31:

- receiving, at a database, biometric data that is based on biometric information taken from a user at a first biometric device and first biometric device data indicative of a capability of the first biometric device;

- upon a successful authorization, locating second biometric device data indicative of a capability of the second biometric device;

- determining whether the first biometric device data indicates that the capability of the first biometric device is superior to the capability of the second biometric device; and

- upgrading said registered biometric data associated with said user record using said received biometric data.

Bianco discloses a method for utilizing biometric measurements for the authentication of users to enterprise resources. *See* Bianco at Abstract. Bianco discloses that a biometric server stores collections of biometric templates, biometric policies, biometric groups, biometric device IDs, user IDs, computer IDs and application IDs. *See id.* at 17: 38-41. A unique biometric template is created and stored in the biometric server each time a user enrolls on a different biometric device. *See id.* at 17:41-44. Biometric groups, which represent a way of combining one or more users that need access to the same set of resources, are also stored in the biometric server. *See id.* at 18:8-11. Each biometric group may be assigned a particular biometric policy that is also stored in the biometric server. *See id.* at 18:18-43. Once it is known which biometric policy will be applied, a biometric template is created for each biometric device associated with the biometric policy by enrolling the user in each device. *See id.* at 19:27-34. Moreover, Bianco teaches that there is one biometric template for each biometric device ID. *See id.* at 24:9-10. As such, Bianco teaches assigning biometric templates based on a biometric group or policy assigned for a particular user and to a particular device.

In contrast, claim 31 requires receiving, at a database, biometric data that is based on biometric information taken from a user at a first biometric device and first biometric device data indicative of a capability of the first biometric device. Bianco merely teaches receiving biometric measurements, which are used to generate a biometric template. Bianco does not teach or suggest receiving data pertaining to the first biometric device. In particular, Bianco does not teach or suggest receiving data indicative of a capability of a first biometric device.

Moreover, claim 31 requires locating second biometric device data indicative of a capability of the second biometric device upon a successful authorization. As mentioned above,

-14-

Bianco merely teaches locating a registered biometric template. Bianco does not teach or suggest locating second biometric device data pertaining to the second biometric device. More particularly, Bianco does not teach or suggest locating second biometric device data indicative of a capability of the second biometric device.

Furthermore, claim 31 requires determining whether the first biometric device data indicates that the capability of the first biometric device is superior to the capability of the second biometric device. Bianco teaches that biometric data may be updated from time to time based on changes in the user's biometric characteristics (due to aging, weight gain or loss, etc.). *See* Bianco at 28:43-52. However, Bianco does not teach or suggest determining whether biometric **device** data indicates that the capability of a first biometric **device** is superior to the capability of a second biometric **device**. Rather, Bianco merely teaches that more current biometric data may indicate a change in a biometric characteristic of a **user**.

Additionally, claim 31 requires upgrading said registered biometric data associated with said user record using said received biometric data. The Office states that Bianco teaches an equation that combines two values to obtain a TEMP SCORE that is used to authenticate a user via a comparison and that in itself is a combination too. *See* Office Action at 3; Bianco at FIG. 21B (2124, 2126). Applicants respectfully disagree. Bianco teaches generating a biometric score from a first device and prompting the user to utilize another device if the biometric score is insufficient to identify a match. The process can repeat until it receives an accurate score or no additional devices are available. *See* Bianco at 30:66-31:25, FIG. 21B. The user is tested on two or more devices either to provide better authentication or to authorize the user if he fails on the first device. As such, the "score" in Bianco represents a biometric matching score. In other words, the score is utilized as part of the matching process. In contrast, claim 31, requires that a biometric match occur first **before considering whether to upgrade the stored biometric data**. If there is no match, the capability of the second device is never considered.

Therefore, for at least the reasons set forth hereinabove, Applicants submit that claim 31 is allowable over the Examiner-cited prior art. *See* MPEP §2131. Because claim 32 depends from and incorporates all of the limitations of allowable independent claim 31, Applicants submit that claim 32 is likewise allowable over the Examiner-cited prior art. Accordingly,

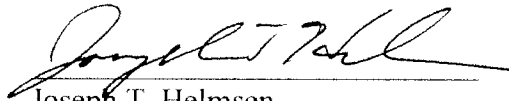Applicants respectfully request that the rejections associated with claims 31 and 32 be withdrawn.

All of the stated grounds of rejection have been properly traversed, accommodated or rendered moot. Applicants therefore respectfully request that the Examiner reconsider and withdraw all presently outstanding rejections. There being no other rejections, Applicants respectfully request that the current application be allowed and passed to issue.

If the Examiner believes for any reason that personal communication will expedite prosecution of this application, I invite the Examiner to telephone me directly.

AUTHORIZATION

The Commissioner is hereby authorized to charge any additional fees which may be required for this Preliminary Amendment, or credit any overpayment, to deposit account no. 50-0436.

Respectfully submitted,
PEPPER HAMILTON LLP

Joseph T. Helmsen
Reg. No. 54,163

Pepper Hamilton LLP
One Mellon Center, 50th Floor
500 Grant Street
Pittsburgh, PA 15219
Telephone: 412.454.5000
Facsimile: 412.281.0717
Date: January 22, 2009